



HGIEL

We Make People Move...

Version 2.0


Information Security Management Policy



Document Owner:


IT - Head

H.G. INFRA ENGINEERING LIMITED

	H.G. Infra Engineering Limited		
	Document No.	Version No.	Date:
	HGIEL/ISMP/19/22	V2.0	01.03.2024
	Information Security Management Policy		

Contents

1. OVERVIEW	2
2. PURPOSE	2
3. APPLICABLE RULES & REGULATIONS.....	2
4. APPLICABILITY	2
5. RESPONSIBILITIES AND POLICY REVIEW.....	2
6. POLICY ELEMENTS.....	2
6.1. Personal Security	3
6.2. Disciplinary action in case of Violation of Information Security Policy	3
6.3. Physical and Environmental Security	3
6.4. Network Security	3
6.5. End-Point Security.....	3
6.6. E-Mail Security	3
6.7. Business Contingency and Disaster Recovery.....	4
6.8. Monitoring of IT Security Systems	4
7. ENFORCEMENT.....	4
8. SPEAK UP.....	4
9. QUERIES	4

	H.G. Infra Engineering Limited		
	Document No.	Version No.	Date:
	HGIEL/ISMP/19/22	V2.0	01.03.2024
Information Security Management Policy			

1. OVERVIEW

The objective of an IT security policy is the preservation of confidentiality, integrity and availability of systems and information used by an organisation's members. An **Information Technology (IT)** policy identifies the rules and procedures for all individuals accessing and using an organization's IT assets and resources.

2. PURPOSE

The purpose of the policy is to minimize risk associated with Data Breach, Cyber Security, e-mail services and defines controls against the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

HGIEL will adhere to the following principles on information security and data privacy:

- Lawfulness, Fairness & Transparency.
- Purpose Limitation.
- Data Minimization.
- Accuracy.
- Storage Limitation.
- Integrity & Confidentiality.
- Accountability.

3. APPLICABLE RULES & REGULATIONS

HGIEL will adhere to the following rules & regulations to ensure information security and data privacy to all its stakeholders:

- Information Technology Act, 2000
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Or Information) Rules, 2011
- Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

4. APPLICABILITY


This policy applies to all employees, working for the company (HGIEL) and its subsidiaries at all levels and grades.

5. RESPONSIBILITIES AND POLICY REVIEW

HGIEL IT Department is responsible for all contents and updates of this policy. Any amendment to document needs to be discussed with Head of IT Department and approved by ESG Council of HGIEL.

6. POLICY ELEMENTS

HGIEL has established policies, objectives and procedures relevant for managing risks and improving information security to deliver results in accordance with its overall policies and objectives.

	H.G. Infra Engineering Limited		
	Document No.	Version No.	Date:
	HGIEL/ISMP/19/22	V2.0	01.03.2024
Information Security Management Policy			

6.1. Personal Security

As per process, on termination of individual employment; terminate information system access, retrieve all organisational information system-related property i.e., Laptop, Mobile, Email ID etc. The access of all resources pertaining to company terminated/blocked by IT department immediately.

6.2. Disciplinary action in case of Violation of Information Security Policy

In case, any employee is found violating any section of the Information Security Policy, disciplinary action is taken according to the Sanction Policy. Adherence to Information Security Policy is considered as an important parameter while evaluating performance of employees.

6.3. Physical and Environmental Security

HGIEL's data centres are hosted in some of the most secure facilities available today in different geographic locations which are far away from each other and in different seismic zones. We use industry best practices that are protected from physical and logical attacks as well as from natural disasters, such as earthquakes, fires, and floods.

6.4. Network Security


HGIEL monitors and update its communication technologies periodically with the goal of providing network security as per industry best practices techniques used to protect the confidentiality, integrity, and authenticity of sensitive and confidential information. Firewall rules and access restrictions are reviewed for appropriateness on a regular basis.

6.5. End-Point Security

Endpoint security is the practice of securing endpoints or entry points of end-user devices such as desktops, laptops devices from being exploited by malicious actors and campaigns. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats.

6.6. E-Mail Security

- Users are prohibited from automatically forwarding email to a third-party email system. Individual messages which are forwarded by the user must not contain confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc.
- The HGIEL email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair, colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any employee should report the matter to their supervisor immediately.
- HGIEL users should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:
 - Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
 - Be suspicious of clickbait titles.
 - Check email and names of unknown senders to ensure they are legitimate.

	H.G. Infra Engineering Limited		
	Document No.	Version No.	Date:
	HGIEL/ISMP/19/22	V2.0	01.03.2024
Information Security Management Policy			

- Some kinds of file are more likely to carry viruses. For example, file names including .vbs, .js, .exe, .bat, .cmd or .lnk extensions.
- Compressed files (containing .zip, .arc or .cab) may also contain such file types.
- Users must not publish or distribute internal mailing lists to non- staff members.
- Excessive email, particularly within your company, can lead to overwork or a tendency to disregard emails, if possible, ignore bulk emails.

6.7. Data Protection

Confidential Information is to be strictly confidential and no employee shall, directly or indirectly, make known such Confidential Information to any person or entity or permit such Confidential Information to be disclosed or made known to any person or entity, in each case either inside or otherwise.

6.8. Business Contingency and Disaster Recovery

HGIEL has established a Disaster Recovery Plan to minimize downtime of the critical business process, and recovery within required and agreed business timescales in the event of a disaster. To prevent data loss due to human error, its critical system application and databases are backed up every day in an automated fashion. Disaster recovery System (DR) is planned and under process of implementation for further data security.

6.9. Monitoring of IT Security Systems


HGIEL's team ensures regular and continuous monitoring by conducting periodic assessments, reviews of company's Information Security Systems for smooth functioning of IT systems.

7. ENFORCEMENT

All HGIEL employees have to adhere to the IT Security Policy and are responsible for implementation of the same in respective areas.

8. SPEAK UP

Employees and other stakeholders are encouraged to report or notify the suspected violations and breaches related to information security and data privacy.

	H.G. Infra Engineering Limited		
	Document No.	Version No.	Date:
	HGIEL/ISMP/19/22	V2.0	01.03.2024
Information Security Management Policy			

9. QUERIES

All are encouraged to raise any concerns or grievances or any questions about the provisions detailed in this document, please contact:

IT - Head

H.G. Infra Engineering Limited

Corporate Office, III Floor, Sheel Mohar Plaza, A-1, Tilak Marg, C-Scheme, Jaipur, Rajasthan - 302001

Board: +91-141-4106 040 / 41

Fax: +91-141 - 4106 044

Mail: isms@hginfra.com

* * * * *

Approved by the Board of Directors
(Amended w.e.f. March 01, 2024)